

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1 9 9 9 年 9 月 1 日

出 願 番 号

Application Number:

平成 1 1 年特許願第 2 4 7 0 6 0 号

出 願 人

Applicant (s):

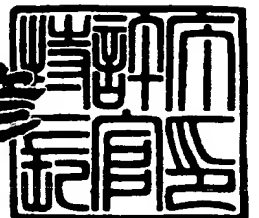
日本電信電話株式会社



2 0 0 0 年 6 月 2 3 日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特 2 0 0 0 - 3 0 4 6 8 3 6

【書類名】 特許願

【整理番号】 NTTH115900

【提出日】 平成11年 9月 1日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

【氏名】 鈴木 幸太郎

【特許出願人】

【識別番号】 000004226

【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100066153

【弁理士】

【氏名又は名称】 草野 卓

【選任した代理人】

【識別番号】 100100642

【弁理士】

【氏名又は名称】 稲垣 稔

【手数料の表示】

【予納台帳番号】 002897

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9806848

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子入札方法及び電子入札方法を記録した記録媒体並びに電子入札装置

【特許請求の範囲】

【請求項1】 開札側の開札者 A に対する入札側の複数の入札者 $B_i (i=1, 2, \dots, n)$ による入札に際して、開札側に備えた開札装置と入札側に備えた入札装置とをネットワークを介して接続し、入札を行なう電子入札方法において、

開札者 A は入札価格表 $\omega_j (j=1, 2, \dots, v, \dots, x)$ および一方向性関数 H を決めて公開する手順 1 と、

入札装置は入札者 B_i の入札価格 ω_{v_i} に対して入札値 $b_{i,1}=b_{i,2}=\dots=b_{i,v_i-1}=\text{no}$ (落札しない)、 $b_{i,v_i}=\text{yes}$ (落札する) を計算する手順 2 と、

入札値に対して一方向性関数 H の連鎖によるコミットメント $L_{i,j}=H(b_{i,j}, L_{i,j+1})$ を計算し、コミットメント $L_{i,1}$ とその署名 σ_i の組 $(L_{i,1}, \sigma_i)$ を入札として開札装置に送信する手順 3 と、

開札装置は送信されてきた入札 $(L_{i,1}, \sigma_i)$ を受信する手順 4 と、

全入札者の入札装置からの入札が揃ったら署名 σ_i が正当であることを検証し、全入札者の入札装置からの入札を公開する手順 5 と、

$j=1$ とする手順 6 と、

入札装置からの入札値 $(b_{i,j}, L_{i,j+1})$ を受信し、全入札者の入札値が揃ったらコミットメント $L_{i,j}$ の正当性 $L_{i,j}=H(b_{i,j}, L_{i,j+1})$ を検証し、全入札値 $\{(b_{i,j}, L_{i,j+1})\}$ を公開する手順 7 と、

全ての i に対して入札値 $b_{i,j}=\text{no}$ なら $j=j+1$ として手順 7 へ戻る手順 8 と、

ある i に対して入札値 $b_{i,j}=\text{yes}$ なら B_i を落札者、 ω_j を落札価格として決定すると共に公開する手順 9 とを備えた

改竄などの不正がなく落札者および落札価格が正当であることを全入札者が検証可能であり、落札者以外の入札価格を秘匿し、一方向性関数の連鎖によるコミットメントを用いることにより効率的に入札が実現できること

を特徴とする電子入札方法。

【請求項 2】 開札側の開札者 A に対する入札側の複数の入札者 $B_i (i=1, 2, \dots, n)$

による入札に際して、開札側に備えた開札装置と入札側に備えた入札装置とをネットワークを介して接続し、入札を行なう電子入札方法において、

開札者 A は入札価格表 $\omega_j (j=1, 2, \dots, v, \dots, x)$ および一方向性関数 H を決めて公開する手順 1 と、

入札装置は入札者 B_i の入札価格 ω_{v_i} に対して入札値 $b_{i,1}=b_{i,2}=\dots=b_{i,v_i-1}=\text{no}$ (落札しない)、 $b_{i,v_i}=\text{yes}$ (落札する) を計算する手順 2 と、

入札値に対して一方向性関数 H の連鎖によるコミットメント $L_{i,j}=H(b_{i,j}, L_{i,j+1})$ を計算し、コミットメント $L_{i,1}$ とその署名 σ_i の組 $(L_{i,1}, \sigma_i)$ を入札として開札装置に送信する手順 3 と、

開札装置は送信されてきた入札 $(L_{i,1}, \sigma_i)$ を受信する手順 4 と、

全入札者の入札装置からの入札が揃ったら署名 σ_i が正当であることを検証し、全入札者の入札装置からの入札を公開する手順 5 と、

$j=1$ とする手順 6 と、

入札装置からの入札値 $(b_{i,j}, L_{i,j+1})$ を受信し、全入札者の入札値が揃ったらコミットメント $L_{i,j}$ の正当性 $L_{i,j}=H(b_{i,j}, L_{i,j+1})$ を検証し、全入札値 $\{(b_{i,j}, L_{i,j+1})\}$ を公開する手順 7 と、

全ての i に対して入札値 $b_{i,j}=\text{no}$ なら $j=j+1$ として手順 7 へ戻る手順 8 と、

ある i に対して入札値 $b_{i,j}=\text{yes}$ なら B_i を落札者、 ω_j を落札価格として決定すると共に公開する手順 9 とを備えた

改竄などの不正がなく落札者および落札価格が正当であることを全入札者が検証可能であり、落札者以外の入札価格を秘匿し、一方向性関数の連鎖によるコミットメントを用いることにより効率的に入札を実現できること

を特徴とする電子入札方法を記録した記録媒体。

【請求項 3】 入札装置は入札者 $B_i (i=1, 2, \dots, n)$ が入札価格表 $\omega_j (j=1, 2, \dots, v, \dots, x)$ から選択した入札価格 ω_{v_i} に対して入札値 $b_{i,1}=b_{i,2}=\dots=b_{i,v_i-1}=\text{no}$ (落札しない)、 $b_{i,v_i}=\text{yes}$ (落札する) を計算する手順 1 と、

入札値 $b_{i,j}$ に対して一方向性関数 H の連鎖によるコミットメント $L_{i,j}=H(b_{i,j}, L_{i,j+1})$ を計算し、入札値 $(b_{i,j}, L_{i,j+1})$ を開札装置に送信する手順 2 と、コミットメント $L_{i,1}$ とその署名 σ_i の組 $(L_{i,1}, \sigma_i)$ を入札として開札装置に

送信する手順 3 とを備えたこと

を特徴とする入札方法。

【請求項 4】 入札装置は入札者 $B_i (i=1, 2, \dots, n)$ が入札価格表 $\omega_j (j=1, 2, \dots, v, \dots, x)$ から選択した入札価格 ω_{v_i} に対して入札値 $b_{i,1}=b_{i,2}=\dots=b_{i,v_i-1}=\text{no}$ (落札しない)、 $b_{i,v_i}=\text{yes}$ (落札する) を計算する手順 1 と、

入札値 $b_{i,j}$ に対して一方向性関数 H の連鎖によるコミットメント $L_{i,j}=H(b_{i,j}, L_{i,j+1})$ を計算し、入札値 $(b_{i,j}, L_{i,j+1})$ を開札装置に送信する手順 2 と、

コミットメント $L_{i,1}$ とその署名 σ_i の組 $(L_{i,1}, \sigma_i)$ を入札として開札装置に送信する手順 3 とを備えたこと

を特徴とする入札方法を記録した記録媒体。

【請求項 5】 開札装置は入札者 $B_i (i=1, 2, \dots, n)$ から送信された入札 $(L_{i,1}, \sigma_i)$ [ただし、入札値 $b_{i,1}$ は入札価格表を $\omega_j (j=1, 2, \dots, v, \dots, x)$ とした場合の ω_1 に対する入札値 (yes : 落札する、no : 落札しない)、 $L_{i,1}=H(b_{i,1}, L_{i,2})$ は入札値 $b_{i,1}$ のコミットメント、 σ_i はコミットメント $L_{i,1}$ の署名] を受信する手順 1 と、

全入札者の入札装置からの入札が揃ったら署名 σ_i が正当であることを検証し、全入札者の入札装置からの入札を公開する手順 2 と、

$j=1$ とする手順 3 と、

入札装置からの入札値 $(b_{i,j}, L_{i,j+1})$ を受信し、全入札者の入札値が揃ったらコミットメント $L_{i,j}$ の正当性 $L_{i,j}=H(b_{i,j}, L_{i,j+1})$ を検証し、全入札値 $\{(b_{i,j}, L_{i,j+1})\}$ を公開する手順 4 と、

全ての i に対して入札値 $b_{i,j}=\text{no}$ なら $j=j+1$ として手順 4 へ戻る手順 5 と、

ある i に対して入札値 $b_{i,j}=\text{yes}$ なら B_i を落札者、 ω_j を落札価格として決定すると共に公開する手順 6 とを備えたこと

を特徴とする開札方法。

【請求項 6】 開札装置は入札者 $B_i (i=1, 2, \dots, n)$ から送信された入札 $(L_{i,1}, \sigma_i)$ [ただし、入札値 $b_{i,1}$ は入札価格表を $\omega_j (j=1, 2, \dots, v, \dots, x)$ とした場合の ω_1 に対する入札値 (yes : 落札する、no : 落札しない)、 $L_{i,1}=H(b_{i,1}, L_{i,2})$ は入札値 $b_{i,1}$ のコミットメント、 σ_i はコミットメント $L_{i,1}$ の署名] を受信す

る手順 1 と、

全入札者の入札装置からの入札が揃ったら署名 σ_i が正当であることを検証し、
全入札者の入札装置からの入札を公開する手順 2 と、

$j=1$ とする手順 3 と、

入札装置からの入札値 $(b_{i,j}, L_{i,j+1})$ を受信し、全入札者の入札値が揃ったら
コミットメント $L_{i,j}$ の正当性 $L_{i,j} = H(b_{i,j}, L_{i,j+1})$ を検証し、全入札値
 $\{(b_{i,j}, L_{i,j+1})\}$ を公開する手順 4 と、

全ての i に対して入札値 $b_{i,j} = \text{no}$ なら $j=j+1$ として手順 4 へ戻る手順 5 と、

ある i に対して入札値 $b_{i,j} = \text{yes}$ なら B_i を落札者、 ω_j を落札価格として決定す
ると共に公開する手順 6 とを備えたこと

を特徴とする開札方法を記録した記録媒体。

【請求項 7】 電子入札装置は、ネットワークを介して接続された入札装置と開
札装置から構成され、

入札装置は、入札価格選択手段、入札値計算手段、コミットメント計算手段、
署名計算手段及び一方向性関数記憶手段とから構成され、

入札者 $B_i (i=1, 2, \dots, n)$ は入札価格選択手段により入札価格表 $\omega_j (j=1, 2, \dots, v, \dots, x)$ から入札価格 ω_{vi} を選択し、入札値計算手段は、入札価格 ω_{vi} に対して
入札値 $b_{i,1} = b_{i,2} = \dots = b_{i,vi-1} = \text{no}$ (落札しない)、 $b_{i,vi} = \text{yes}$ (落札する) を
計算し、コミットメント計算手段は、一方向性関数 H の連鎖を用いて入札値 $b_{i,j}$
に対するコミットメント $L_{i,j} = H(b_{i,j}, L_{i,j+1})$ を計算し、署名計算手段は、
コミットメント $L_{i,1}$ に対しての署名 σ_i を計算し、そして、入札装置は、入札 $(L_{i,1}, \sigma_i)$ を開札装置へ送信し、開札装置が署名 σ_i が正当であることを検証し、
全入札を公開し、さらに、入札装置は、入札値 $(b_{i,j}, L_{i,j+1})$ を開札装置へ送
信し、開札装置がコミットメント $L_{i,j}$ の正当性 $L_{i,j} = H(b_{i,j}, L_{i,j+1})$ を検証
し、この入札値の公開を確認したら、順次、入札値 $(b_{i,j+1}, L_{i,j+2})$ 、 $(b_{i,j+2}, L_{i,j+3})$ 、 \dots を送信すると共に、

開札装置は、署名検証手段、全入札公開手段、コミットメント検証手段、全入
札値公開手段、落札計算手段、落札者・落札価格公開手段及び一方向性関数記憶
手段とから構成され、

署名検証手段と全入札公開手段は、入札 $(L_{i,1}, \sigma_i)$ を受信して、署名 σ_i の正当性を検証すると共に、全入札を公開し、コミットメント検証手段と全入札値公開手段は、入札値 $(b_{i,j}, L_{i,j+1})$ を受信し、コミットメント $L_{i,j}$ の正当性 $L_{i,j} = H(b_{i,j}, L_{i,j+1})$ を検証すると共に、全入札値 $\{(b_{i,j}, L_{i,j+1})\}$ を公開し、また、落札計算手段は、全ての i に対して入札値 $b_{i,j} = \text{no}$ ならば、 $j = j+1$ としてコミットメント検証手段、全入札値公開手段に送信し、ある i に対して入札値 $b_{i,j} = \text{yes}$ ならば、落札と判断して落札者・落札価格公開手段に送信し、落札者・落札価格公開手段は落札者、落札価格を公開し、

改竄などの不正がなく落札者および落札価格が正当であることを全入札者が検証可能であり、落札者以外の入札価格を秘匿し、一方向性関数の連鎖によるコミットメントを用いることにより効率的に入札を実現できること

を特徴とする電子入札装置。

【請求項 8】 入札装置は、入札価格選択手段、入札値計算手段、コミットメント計算手段、署名計算手段及び一方向性関数記憶手段とから構成され、

入札者 $B_i (i=1, 2, \dots, n)$ は入札価格選択手段により入札価格表 $\omega_j (j=1, 2, \dots, v, \dots, x)$ から入札価格 ω_{vi} を選択し、入札値計算手段は、入札価格 ω_{vi} に対して入札値 $b_{i,1} = b_{i,2} = \dots = b_{i,vi-1} = \text{no}$ (落札しない)、 $b_{i,vi} = \text{yes}$ (落札する) を計算し、コミットメント計算手段は、一方向性関数 H の連鎖を用いて入札値 $b_{i,j}$ に対するコミットメント $L_{i,j} = H(b_{i,j}, L_{i,j+1})$ を計算し、署名計算手段は、コミットメント $L_{i,1}$ に対しての署名 σ_i を計算し、そして、入札装置は、入札 $(L_{i,1}, \sigma_i)$ を開札装置へ送信し、開札装置が署名 σ_i が正当であることを検証し、この入札を公開し、さらに、入札装置は、入札値 $(b_{i,j}, L_{i,j+1})$ を開札装置へ送信し、開札装置がコミットメント $L_{i,j}$ の正当性 $L_{i,j} = H(b_{i,j}, L_{i,j+1})$ を検証し、この入札値の公開を確認したら、順次、入札値 $(b_{i,j+1}, L_{i,j+2})$ 、 $(b_{i,j+2}, L_{i,j+3})$ 、 \dots を送信すること

を特徴とする入札装置。

【請求項 9】 開札装置は、署名検証手段、全入札公開手段、コミットメント検証手段、全入札値公開手段、落札計算手段、落札者・落札価格公開手段、一方向性関数記憶手段及び入札価格表 $\omega_j (j=1, 2, \dots, v, \dots, x)$ とから構成され、

署名検証手段と全入札公開手段は、入札者 $B_i (i=1, 2, \dots, n)$ の入札 $(L_{i,1}, \sigma_i)$ [ただし、入札値 $b_{i,1}$ は ω_1 に対する入札値 (yes: 落札する、no: 落札しない)、 $L_{i,1}$ は入札値 $b_{i,1}$ のコミットメント、 σ_i はコミットメント $L_{i,1}$ の署名] を受信して、署名 σ_i の正当性を検証すると共に、全入札 $\{ (L_{i,1}, \sigma_i) \}$ を公開し、コミットメント検証手段と全入札値公開手段は、入札値 $(b_{i,j}, L_{i,j+1})$ を受信し、コミットメント $L_{i,j}$ の正当性 $L_{i,j} = H(b_{i,j}, L_{i,j+1})$ を検証すると共に、全入札値 $\{ (b_{i,j}, L_{i,j+1}) \}$ を公開し、また、落札計算手段は、全ての i に対して入札値 $b_{i,j} = \text{no}$ ならば、 $j=j+1$ としてコミットメント検証手段、全入札値公開手段に送信し、ある i に対して入札値 $b_{i,j} = \text{yes}$ ならば、落札と判断して落札者、落札価格公開手段に送信し、落札者・落札価格公開手段は落札者・落札価格を公開すること

を特徴とする開札装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報セキュリティ技術の応用技術に関するものであり、インターネットなどの通信ネットワーク上に分散配置された複数の入札者が、電子的な通信を利用して入札を行う、電子入札装置並びに電子入札方法及び電子入札方法を記録した記録媒体に関する。

【0002】

【従来の技術】

従来方式の代表的な例として、宮崎、櫻井による電子入札方式(S.Miyazaki, K. Sakurai, 公開掲示板を用いた秘策可能な電子入札システム、SCIS' 99 41-46 (1999))がある。

【0003】

【発明が解決しようとする課題】

従来方式においては否認不可署名（入札者がある価格で入札していないことを証明できる署名方式）によるコミットメントが用いられていたが、否認不可署名は署名の作成／確認／否認手順に多くの計算および通信を必要とするため効率が

よくないという問題点があった。

【0004】

【課題を解決するための手段】

本発明が提案する電子入札装置及び方法は、一方向性関数の連鎖によるコミットメントを用いて構成されているため、一方向性関数として例えばSHA-1などの実用的な一方向性関数を用いることにより、従来方式よりも効率的な入札方法を実現している。

【0005】

【発明の実施の形態】

以下では、本発明の一実施例について説明する。

図1は、本発明の全体構成を示す図である。入札者 B_1, B_2, \dots, B_n (100)が開札者A(200)と通信路(300)を介して結合されている。

実施例1

図2に示すように、まず開札者Aは「前処理」を行い、次に各入札者 B_i ($i=1, \dots, n$)は「入札手順」(110-150)により入札を行ない、最後に開札者Aは「開札手順」(210-250)により開札を行なう。

【0006】

図3に入札者 B_i (100)の入札手順のブロック図を示す。

図4に開札者A(200)の開札手順のブロック図を示す。

〔前処理〕

開札者Aは入札価格表 $\{\omega_1, \dots, \omega_{v-1}, \omega_v, \dots, \omega_x\}$ （例えば、中古車の販売で{100万円, ..., 60万円, 50万円, ..., 10万円}、すなわち、開札者は価格100万円から10万円の範囲と具体的な入札価格を提示する。）および一方向性関数

$$H: \{0,1\}^s \times \{0,1\}^t \rightarrow \{0,1\}^t$$

（ただし、 $\{0,1\}^s$ は $\{0,1\}$ の集合から成る s ビットのビット列の全体集合、 $\{0,1\}^t$ は $\{0,1\}$ の集合から成る t ビットのビット列の全体集合を示す。）を決めて公開する。実際には、一方向性関数としてSHA-1などの実用的な一方向性関数を用いる。また、no（落札しないメッセージ）、yes（落札するメッセージ

) $\in \{0,1\}^S$ を公開する。

[入札手順]

入札者 B_i は、図 4 に示す入札手順(110-150)により入札を行う。

(ステップ110)

入札者 B_i は、入札価格表 $\{\omega_1, \dots, \omega_{v-1}, \omega_v, \dots, \omega_x\}$ から入札価格 ω_{vi} を選択する (例えば、50万円)。

(ステップ120)

入札価格 ω_{vi} に対する入札値

$\neg no \in \{0,1\}^S \quad (1 \leq j \leq vi-1) \quad (\text{落札しない})$

$b_{i,j} = |$

$\neg yes \in \{0,1\}^S \quad (j = 1) \quad (\text{落札する})$

を計算する。

【0007】

(例えば、入札者 B_i は、60万円、 \dots 、100万円では落札を希望せず、50万円で希望する場合には、 $\{\omega_1$ (100万円) , \dots , ω_{v-1} (60万円) , ω_{vi} (50万円) } に対する $\{b_{i,1}, \dots, b_{i,vi-1}, b_{i,vi}\}$ は $\{no, \dots, no, yes\}$ となる。

)

(ステップ130)

入札値 $b_{i,j}$ に対するコミットメント

$L_{i,j} = H(b_{i,j}, L_{i,j+1}) \quad (1 \leq j \leq vi)$

を計算する。

【0008】

(上記の計算は、 $\{0,1\}^t$ からランダムに選んだ $L_{i,vi+1}$ を初期値として、 $L_{i,vi} = H(b_{i,vi}, L_{i,vi+1})$, \dots , $L_{i,2} = H(b_{i,2}, L_{i,3})$, $L_{i,1} = H(b_{i,1}, L_{i,2})$ により行う。)

(ステップ140)

$b_{i,1}$ に対するコミットメント $L_{i,1}$ に対して、署名 $\sigma_i = \text{Sig}_{B_i}(L_{i,1})$ を計算する。

(この署名により入札は確かに入札者 B_i が行ったものであることがわかる。)

(ステップ150)

$b_{i,1}$ に対するコミットメント $L_{i,1}$ とその署名 σ_i の組 $(L_{i,1}, \sigma_i)$ を入札として、開札者 A に送信する。

[開札手順]

開札者 A は、図 4 に示す開札手順(210-250)により開札を行い、全入札者 $B_i (i=1,2,\dots,n)$ に入札値 $\{b_{1,1}, b_{1,2}, \dots, b_{1,v_1}\}$ (入札者 B_1) , \dots , $\{b_{i,1}, b_{i,2}, \dots, b_{i,v_i}\}$ (入札者 B_i) , \dots , $\{b_{n,1}, b_{n,2}, \dots, b_{n,v_n}\}$ (入札者 B_n)] を順に送信させて開札手順(210-250)により開札を行う。

(ステップ 2 1 0)

入札者 B_i から入札 $(L_{i,1}, \sigma_i)$ を受信し、全入札者 $B_i (i=1,2,\dots,n)$ からの入札 $\{L_{i,1}, \sigma_i\} (i=1,2,\dots,n)$ が揃ったら、署名 σ_i の正当性を検証し、全入札 $\{(L_{i,1}, \sigma_i)\} (i=1,2,\dots,n)$ を公開する。(例えば、 $\{(L_{1,1}, \sigma_1), \dots, (L_{n,1}, \sigma_n)\}$ を表示装置に表示して公開する。(この表示からは具体的な入札価格は知ることはできない。ただし、その後、入札価格等が改竄されれば $\{(L_{1,1}, \sigma_1), \dots, (L_{n,1}, \sigma_n)\}$ が変わり、改竄されたことがわかる。)

(ステップ220)

$j=1$ (すなわち、入札価格 ω_1 に対する全入札者 $B_i (i=1,2,\dots,n)$ の入札値 $\{b_{1,1}, b_{2,1}, \dots, b_{n,1}\}$ 、 $j=2$ (すなわち、入札価格 ω_2 に対する全入札者 $(B_1, \dots, B_i, \dots, B_n)$ の入札値 $\{b_{1,2}, b_{2,2}, \dots, b_{n,2}\}$ 、 \dots を順に公開すると共に、 $j=1,2,\dots$ 毎に以下のステップ (230-250)を行う。

(ステップ230)

入札者 B_i から入札値 $(b_{i,j}, L_{i,j+1})$ を受信し、全入札値 $\{(b_{i,j}, L_{i,j+1})\} (i=1,2,\dots,n)$ が揃ったら、コミットメントの正当性

$$L_{i,j} = H(b_{i,j}, L_{i,j+1})$$

を検証し、全入札値 $\{(b_{i,j}, L_{i,j+1})\} (i=1,2,\dots,n)$ を公開する。

(ステップ240)

全ての i に対して入札値 $b_{i,j} = \text{no}$ なら、 $j=j+1$ として (ステップ230) へ戻る。

(ステップ250)

ある i に対して入札値 $b_{i,j} = \text{yes}$ なら、 $v=j$ として、 B_i を落札者、 ω_v を落札価

格として公開する。

【0009】

実施例 2

図 5 は、本発明の電子入札装置のブロック図を示す。

電子入札装置 1 は、入札装置 2 と開札装置 3 から構成される。

入札装置 1 は、入札価格選択手段 4、入札値計算手段 5、コミットメント計算手段 6、署名計算手段 7 及び一方向性関数記憶手段 8 とから構成される。

【0010】

入札者 $B_i (i=1, 2, \dots, n)$ は、公開されている入札価格表 $\omega_j (j=1, 2, \dots, v, \dots, x)$ 9 を参照して入札価格選択手段 4 により入札価格 ω_{vi} を選択する。入札値計算手段 5 は、入札価格 ω_{vi} に対する入札価格 ω_{vi} に対して入札値 $b_{i,1}=b_{i,2}=\dots=b_{i,vi-1}=no$ (落札しない)、 $b_{i,vi}=yes$ (落札する) を計算する。コミットメント計算手段 6 は、一方向性関数 H の連鎖を用いて入札値 $b_{i,j}$ に対するコミットメント $L_{i,j}=H(b_{i,j}, L_{i,j+1})$ を計算する。署名計算手段 7 は、コミットメント $L_{i,1}$ に対しての署名 σ_i を計算する。そして、入札装置 2 は、入札 $(L_{i,1}, \sigma_i)$ を開札装置へ送信し、開札装置が署名 σ_i が正当であることを検証すると共に、全入札を公開し、さらに、入札装置は、入札値 $(b_{i,j}, L_{i,j+1})$ を開札装置へ送信し、開札装置がコミットメント $L_{i,j}$ の正当性を検証し、この入札値の公開を確認したら、順次、入札値 $(b_{i,j+1}, L_{i,j+2})$ 、 $(b_{i,j+2}, L_{i,j+3})$ 、 \dots を送信する。

【0011】

開札装置 3 は、署名検証手段 10-1、全入札公開手段 10-2、コミットメント検証手段 11-1、全入札値公開手段 11-2、落札計算手段 12、落札者・落札価格公開手段 13 及び一方向性関数記憶手段 8 とから構成される。

署名検証手段 10-1 と全入札公開手段 10-2 は、入札 $(L_{i,1}, \sigma_i)$ を受信して、署名 σ_i の正当性を検証すると共に、全入札 $\{(L_{i,1}, \sigma_i)\} (i=1, 2, \dots, n)$ を公開する。コミットメント検証手段 11-1 と全入札値公開手段 11-2 は、入札値 $(b_{i,j}, L_{i,j+1})$ を受信し、一方向性関数 H を用いてコミットメント $L_{i,j}$ の正当性を検証すると共に、全入札値 $\{(b_{i,j}, L_{i,j+1})\} (i=1, 2, \dots, n)$ を公開する。また、

落札計算手段12は、入札値 $b_{i,j}$ を受信し、全ての i に対して入札値 $b_{i,j} = \text{no}$ ならば、 $j=j+1$ としてコミットメント検証手段11-1、全入札値公開手段11-2に送信し、ある i に対して入札値 $b_{i,j} = \text{yes}$ ならば、落札と判断して落札者・落札価格公開手段13に送信し、落札者・落札価格を公開する。

〔例外処理〕

入札値 $(b_{i,j}, L_{i,j+1})$ を公開しない入札者 B_i がいる場合、その入札者 B_i を除いて、再度入札をやり直す。（現実には、公開しない入札者 B_i に対しては、さらに預かり金没収などの罰則を設けて対処することとなる。）

【0 0 1 2】

〔発明の効果〕

本発明で提案する電子入札方法および装置は、一方向性関数の連鎖によるコミットメントを用いて構成されているためSHA-1などの実用的な一方向性関数を用いることにより、否認不可署名によるコミットメントを用いていた従来方式よりも効率的な電子入札方法及び装置を実現している。

【0 0 1 3】

さらに、電子入札方法及び装置として必要な次のような性質を備えている。

〔正確性〕

順に入札を開示していくので、最小の v に対応する ω_v で入札した入札者が落札する。

〔検証可能性〕

入札 $\{b_{i,1}, b_{i,2}, \dots, b_{i,v}\}$ とコミットメント $\{L_{i,1}, L_{i,2}, \dots, L_{i,v+1}\}$ は公開されているので、だれでも改竄の検証をすることができる。

〔公平性〕

開札以前に公開されているのはコミットメント $L_{i,1}$ のみなので、開札までは他の入札者の入札価格はわからない。

〔価格秘匿性〕

落札者が出たところで開札は終了し、落札者が出てきた以降の入札 $\{b_{i,v+1}, b_{i,v+2}, \dots, b_{i,v_i}\}$ は公開されないの、落札価格以外の入札価格は秘匿されている。

〔否認不可性〕

コミットメント $L_{i,1}$ には入札者の署名 $\sigma_i = \text{Sig}_{B_i}(L_{i,1})$ が付いているので否認できない。

〔不正者特定可能性〕

コミットメント $L_{i,j}$ が公開されているので入札 $b_{i,j}$ を偽った者は特定できる。また、一方向性関数 H の一方向性により、コミットメント $L_{i,j}$ を後から改竄することはできない。

【図面の簡単な説明】

【図 1】

本発明の全体構成を示す図。

【図 2】

本発明の全体的な手順を示す図。

【図 3】

入札者 B_i の入札手順のブロック図。

【図 4】

開札者 A の開札手順を示すブロック図。

【図 5】

本発明の電子入札装置のブロック図。

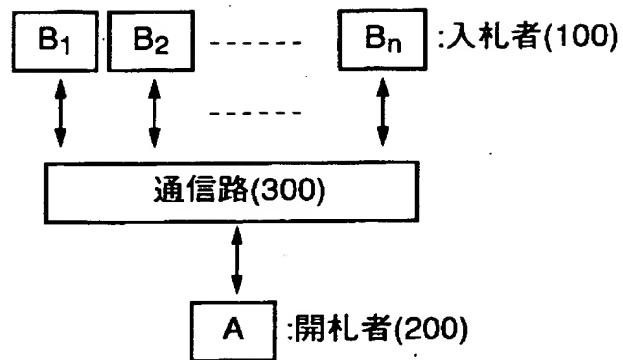
【符号の説明】

- 1 電子入札装置
- 2 入札装置
- 3 開札装置
- 4 入札価格選択手段
- 5 入札値計算手段
- 6 コミットメント計算手段
- 7 署名計算手段
- 8 一方向性関数記憶手段
- 9 入札価格表
- 10-1 署名検証手段

- 10-2 全入札公開手段
- 11-1 コミットメント検証手段
- 11-2 全入札値公開手段
- 12 落札計算手段
- 13 落札者・落札価格公開手段

【書類名】 図面

【図 1】



本発明の全体構成

図 1

【図 2】

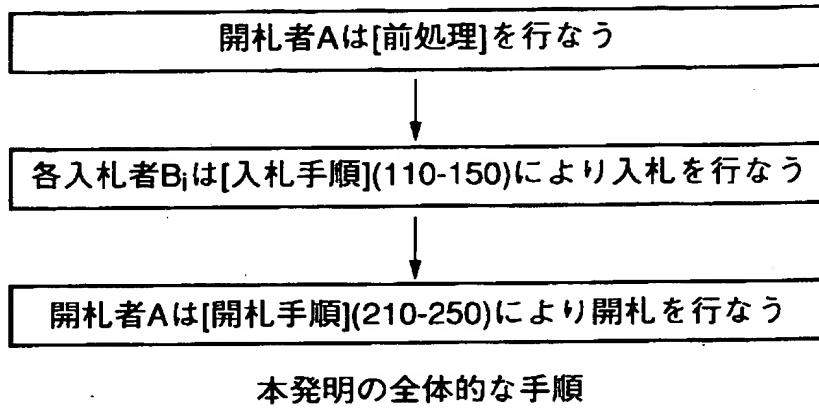


図 2

【図 3】

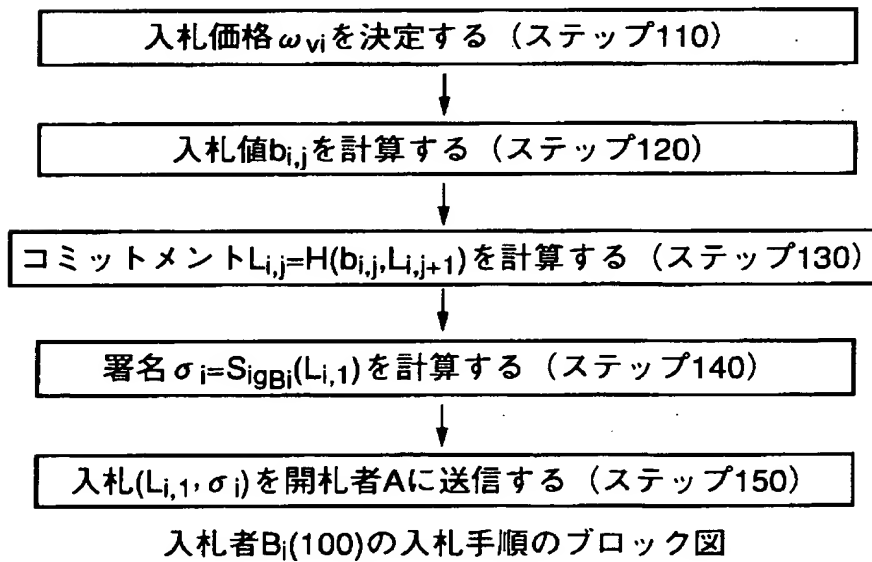


図 3

【図 4】

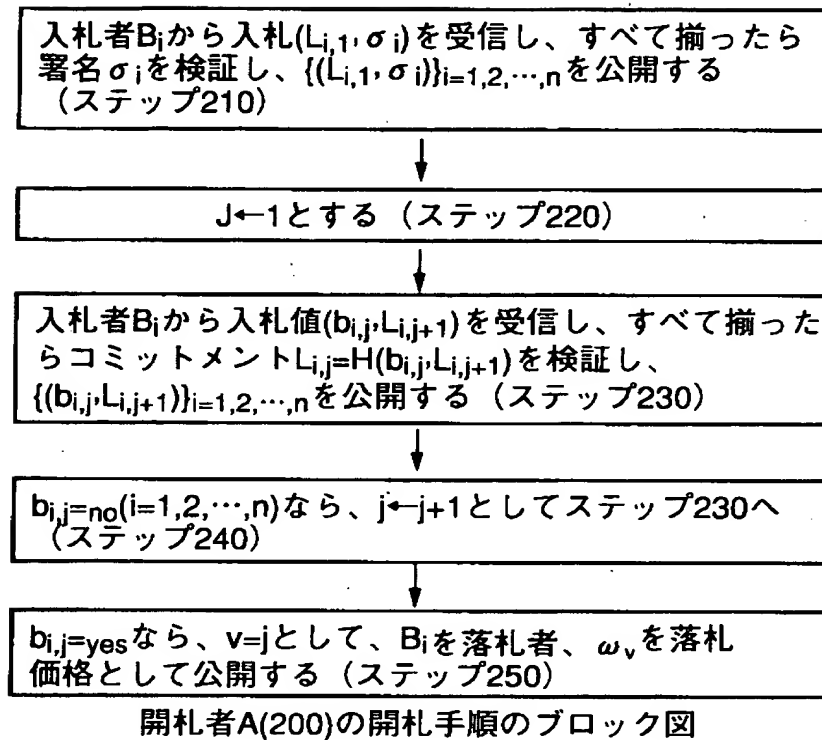


図 4

【図 5】

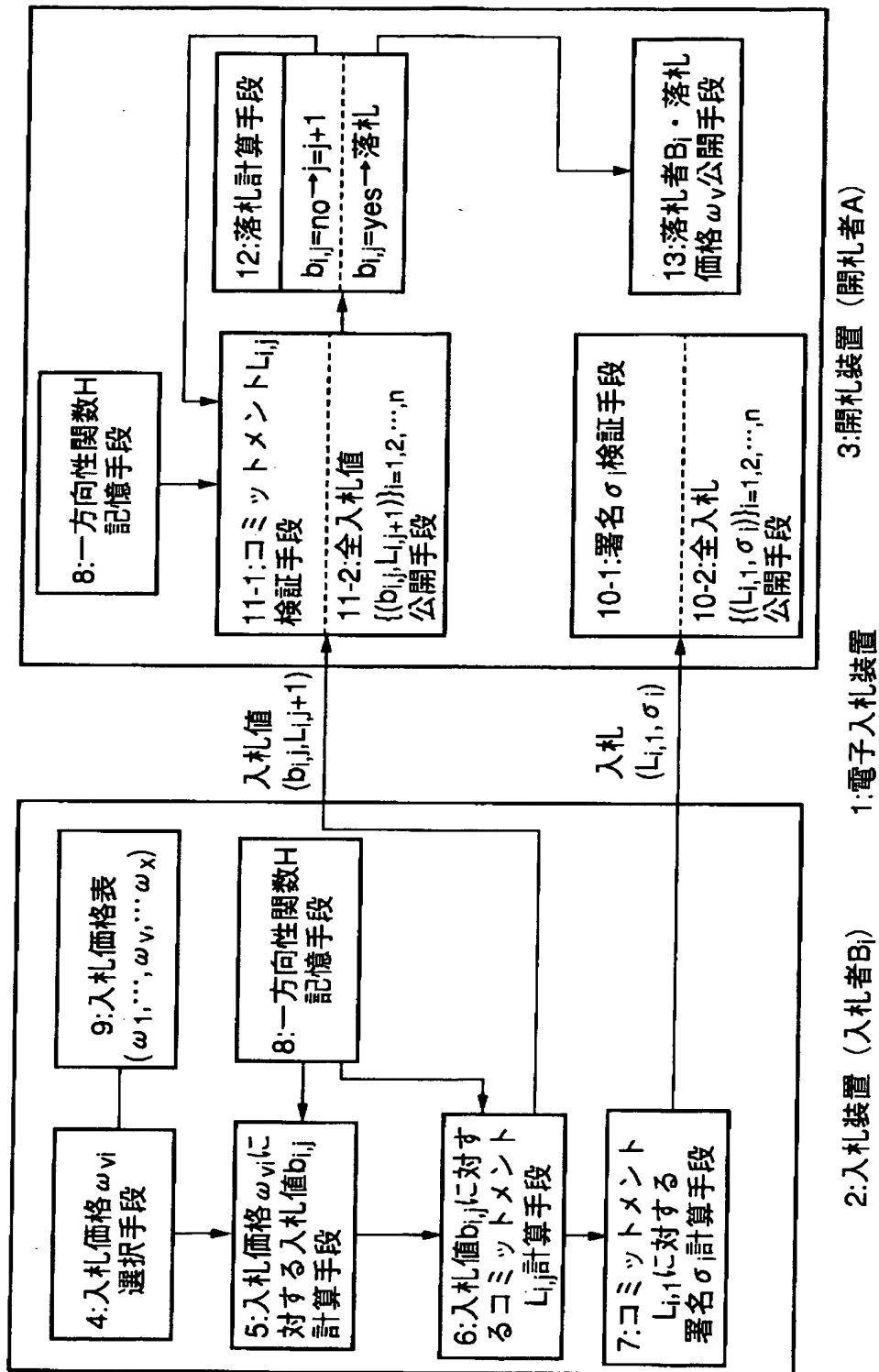


図 5

【書類名】 要約書

【要約】

【課題】 否認不可署名によるコミットメントを用いることなく、改竄などの不正がなく落札者および落札価格が正当であることを全入札者が検証可能であり、落札者以外の入札価格を秘匿することができる電子入札方法を提供する。

【解決手段】 入札装置は入札者の入札価格に対して入札値を計算し、さらに入札値に対して一方向性関数の連鎖によるコミットメントを計算し、コミットメントとその署名の組を入札として開札装置に送信すると共に、開札装置は入札を受信し、全入札者の入札が揃ったら署名が正当であることを検証し、全入札者の入札を公開し、入札装置からの入札値を受信し、全入札者の入札値が揃ったらコミットメントの正当性を検証し全入札値を公開すると共に、落札者と落札価格を決定し、公開する。

【選択図】 図 5

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日	1999年 7月15日
[変更理由]	住所変更
住 所	東京都千代田区大手町二丁目3番1号
氏 名	日本電信電話株式会社